UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

LESLIE LINWOOD RICH, on behalf of himself and other similarly situated individuals, Plaintiff, v. LEMONADE, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Leslie Linwood Rich ("Plaintiff"), individually and on behalf of all others similarly situated, by and through undersigned counsel, brings this class action complaint against Defendant Lemonade, Inc. ("Defendant" or "Lemonade") and alleges as follows:

I. INTRODUCTION

1. Every year, millions of Americans have their most valuable, highly sensitive personal information compromised by unauthorized individuals because corporations prioritize maximizing profits over protecting the sensitive information entrusted to them, leaving the public vulnerable to data disclosures and other data security incidents.

2. In recognition of the sensitivity of driver's license information (and its utility to identity thieves), Congress passed the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721, *et seq.* ("DPPA"), which restricts access to driver's license information, and mandates that private companies may only use that information for limited, enumerated purposes.

3. In the DPPA, Congress specifically defines personal information ("PI") to include driver's license numbers. *See* 18 U.S.C. § 2725(3). Thus, under the DPPA, private companies are

legally required to only access, or provide access to, driver's license numbers for very specific purposes.

4. Threat actors seek out driver's license numbers because they are highly valuable pieces of PI. A driver's license number can be a critical part of a fraudulent, synthetic identity, with reports indicating that the going rate for a stolen identity is about $1,200 on the dark web, and that a stolen or forged driver's license, alone, can sell for around $200.[1] Driver's license numbers are particularly useful to identity thieves for applying for unemployment or other government benefits.

5. Defendant is a provider of private passenger automobile insurance policies and offer coverages to automobile insureds throughout the United States. Defendant markets its insurance policies through its website, https://www.lemonade.com/car, which contains an online quoting platform ("Quote Platform") through which prospective customers can apply for insurance coverage and receive a quote from Defendant online.

6. Despite knowing that driver's license numbers can only be used and disclosed for specific enumerated purposes, Defendant knowingly and willfully designed and implemented a feature on its Quote Platform where an individual's driver's license number would auto-populate in the Quote Platform or otherwise become viewable by the public—after only a bare minimum of publicly available information was entered about an individual (i.e., name, address, etc.)—making the auto-populated driver's license number visible to users of Defendant's Quote Platform, despite the fact that such users had no permissible purpose to access or view driver's license numbers

[1] Lee Mathews, *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes (Apr. 20, 2021, 11:57 A.M. EDT), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=146576a68658.

under the DPPA and Defendants had no way to verify that those auto-populated driver's license numbers were shown to only the individuals to whom they belonged.[2]

7. Defendant did so for its own self-interest: to increase the likelihood that consumers would complete their applications and purchase insurance policies from Defendant through the Quote Platform. By automatically pulling information about consumers' driver's license numbers into the Quote Platform, Defendant sidestepped the process of asking Quote Platform visitors to manually enter their driver's license numbers themselves. By limiting the amount of information such visitors needed to enter in order to receive an insurance quote—by pre-filling that information instead—Defendant reduced the time and effort required to complete the application process in order to sell more insurance but did so at the cost of publicly displaying individuals' highly sensitive driver's license numbers.

8. Nothing about Defendant's underwriting or insurance quoting process required it to auto-populate driver's license numbers on its website. Indeed, Defendant had offered online insurance quotes to applicants long before it incorporated this auto-population feature to its Quote Platform; instead, Defendant added the auto-population feature to gain a competitive advantage in its sales process. That is, the less information requested from the prospective customer, the more likely they are to finish the application and purchase insurance from Defendant. Thus, Defendant's conduct was motivated by its desire to entice customers to complete applications for insurance.

9. By knowingly and intentionally designing and implementing the auto-population feature on its Quote Platform, Defendant knowingly and intentionally obtained, used, and disclosed Plaintiff's and class members' driver's license numbers (and other PI) on its Quote

[2] Jonathan Greig, *Insurance firm Lemonade says breach exposed driver's license numbers,* The Record (Apr. 14, 2025), https://therecord.media/lemonade-insrance-breach-numbers-license

Platform. Defendant's decision made driver's license numbers and PI easily accessible to anyone who entered a prospective customer's basic information.

10. Defendant designed its Quote Platform and website to display driver's license numbers and other PI to any website user who entered basic information about someone, even if it is not the person to whom the sensitive information relates. Defendant did not implement or maintain any effective security processes or systems to prevent unauthorized parties and/or automated bots from using Defendant's website to harvest consumers' PI through its Quote Platform.

11. In essence, in its pursuit of selling more insurance and improving its bottom line, Defendant intentionally created a website that allowed anyone to look up someone's driver's license number and other PI, merely by entering rudimentary information about such a person. Effectively, Defendant posted Plaintiff's and the class members' driver's license numbers and PI on the internet's "windshield" for all digital passersby to see.

12. Unsurprisingly, Defendant's profit-seeking conduct quickly caught the attention of opportunists, who utilized Defendant's Quote Platform to obtain the highly sensitive driver's license numbers and PI of approximately 190,000 consumers, including Plaintiff, over the course of *17 months* (the "Data Disclosure"), which Defendant failed to discover for nearly *two years*—i.e., from when the Data Disclosure began in April 2023 until Defendant discovered it in March 2025.[3]

13. Defendant sent letters to individuals impacted by the Data Disclosure beginning on or about April 10, 2025 (the "Notice"), stating that between "April 2023 and September 2024"

[3] Jonathan Greig, *Insurance firm Lemonade says breach exposed driver's license numbers,* The Record (Apr. 14, 2025), https://therecord.media/lemonade-insrance-breach-numbers-license

"due to a vulnerability in our Online Flow, certain drivers license numbers for identifiable individuals [including Plaintiff] were likely exposed."

14. In the Notice, Defendant acknowledged that driver's license numbers and other PI accessed through the Data Disclosure can be used to conduct various forms of fraud and identity theft and urged impacted individuals to "remain vigilant with respect to reviewing your account statement and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities."

15. Defendant's Notice conveniently omitted that the information, used by the unauthorized third parties to obtain Plaintiff's and Class Members' driver's license numbers and PI from Defendant's Quote Platform, was simply their names, addresses, and other similar contact information publicly available (commonly referred to as "phone book" information) through a simple Google search or accumulated in databases and widely available on the internet.

16. Defendant's Notice explains that the Data Disclosure occurred between April 2023 and September 2024, which means Defendant allowed the disclosure to continue for *seventeen months* and failed to inform Plaintiff and Class Members of the Data Disclosure for *two years*.

17. Defendant sent a Notice to Plaintiff confirming that his sensitive driver's license number was obtained by Defendant, displayed or otherwise disclosed on Defendant's website through the Quote Platform, and ultimately accessed by cybercriminals. Defendant uses the Quote Platform to attract and obtain new business and increase its revenue and profit.

18. As a result of Defendant's intentional conduct in obtaining, using, and disclosing Plaintiff's and Class Members' driver's license numbers and other PI on its Quote Platform for all to see, and the resulting Data Disclosure, Plaintiff's privacy has been invaded, his sensitive driver's license information is now in the hands of unauthorized third parties, and he faces a substantially

increased risk of identity theft and fraud. Accordingly, Plaintiff now must take immediate and time-consuming action to protect himself from identity theft and fraud.

19. To redress Defendant's illegal, self-interested, profit-seeking conduct, Plaintiff brings this class action on behalf of himself and all other individuals ("Class Members") who had their driver's license numbers obtained by Defendant, displayed or otherwise disclosed on Defendant's website through the Quote Platform, used by Defendant to attract and obtain new business and increase its revenue and profit, and ultimately accessed by cybercriminals via the Data Disclosure. Plaintiff, on behalf of and the Class Members, seeks remedies, including monetary damages and injunctive relief (including relief under the federal Declaratory Judgment Act), for negligence, invasion of privacy, and Defendant's violations of the DPPA.

II. PARTIES

20. Plaintiff Leslie Linwood Rich is a resident and citizen of the state of Arizona.

21. Defendant Lemonade, Inc. is a company with its principal place of business in New York City, New York. Defendant, though affiliates, insures private passenger automobiles and provides homeowner and other types of insurance for qualified applicants. Defendant obtained access to Plaintiff's and Class Members' driver's licenses and/or PI in the regular course of its business.

III. JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 as it arises under the laws of the United States, including the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721, *et seq.*

23. This Court also has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367(a).

24. Alternatively, this Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs; the number of members of the proposed Class exceeds 100; and diversity exists because upon information and belief, at least one Class Member and Defendant are citizens of different states.

25. The Court has personal jurisdiction over Defendant because it maintains its headquarters and principal places of business in this District and conducts significant business in this District, thus availing itself of New York's markets by selling auto insurance policies therein; it has sufficient minimum contacts with New York; and a substantial part of the conduct giving rise to Plaintiff's claims occurred in this District.

26. Venue properly lies in this District pursuant to 28 U.S.C. § 1391 because, *inter alia*, a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in, were directed to, and/or emanated from this District; Defendant transacts substantial business and has agents in this District; a substantial part of the conduct giving rise to Plaintiff's claims occurred in this District; and because Defendant resides within this District.

IV. FACTUAL ALLEGATIONS

A. Defendant Collects Vast Amounts of Sensitive PI—including Driver's License Numbers—from Consumers and Third Parties

27. Defendant primarily offers private passenger automobile and home insurance to individuals nationwide. Defendant also offers renters, pet and life insurance.

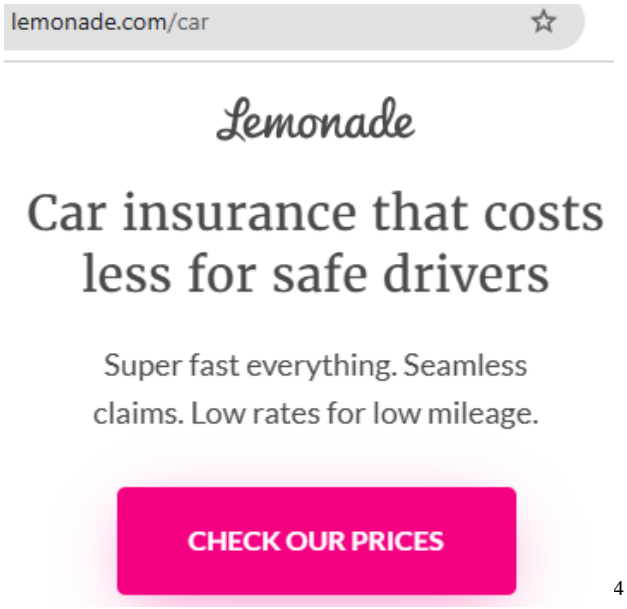
28. Defendant collects and stores vast amounts of PI and sensitive data from prospective clients, current and former customers, and other consumers, as part of its regular business practices, including highly sensitive driver's license numbers, as well as names, aliases, postal addresses, Social Security numbers, bank account numbers, credit card numbers and

medical information. Discovery will show that during the insurance claims process, Defendant also requires submission of similar PI in connection with insurance processing claims, including from individuals who are not Defendant's policyholders but who are involved in a claim being handled by Defendant, such as drivers involved in accidents with Defendant's insureds.

29. Defendant's marketing is primarily through direct response methods in which consumers submit applications for insurance quotes directly to Defendant via the internet or by telephone.

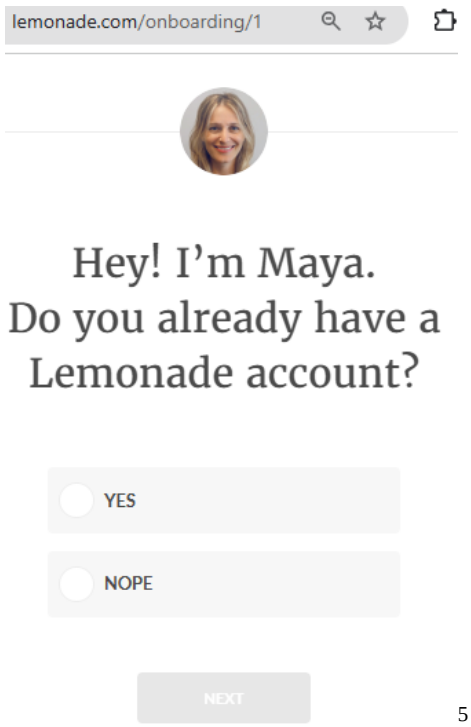
30. Competition for private passenger automobile insurance, which is substantial, tends to focus on price and level of customer service provided.

31. Like other insurance providers, Defendant has an online Quote Platform available to all persons capable of accessing it via the internet: https://www.lemonade.com/car. Visitors to Defendant's Quote Platform can get a quote instantly after providing basic PI in a series of pages on Defendant's website, as depicted below:

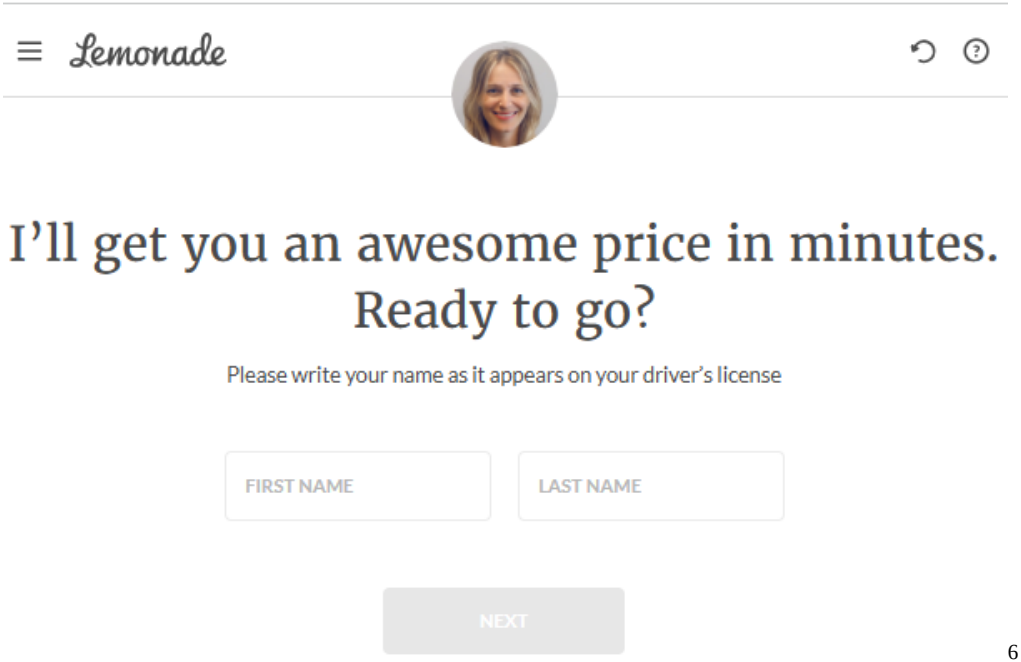


[4]

[4] https://www.lemonade.com/car

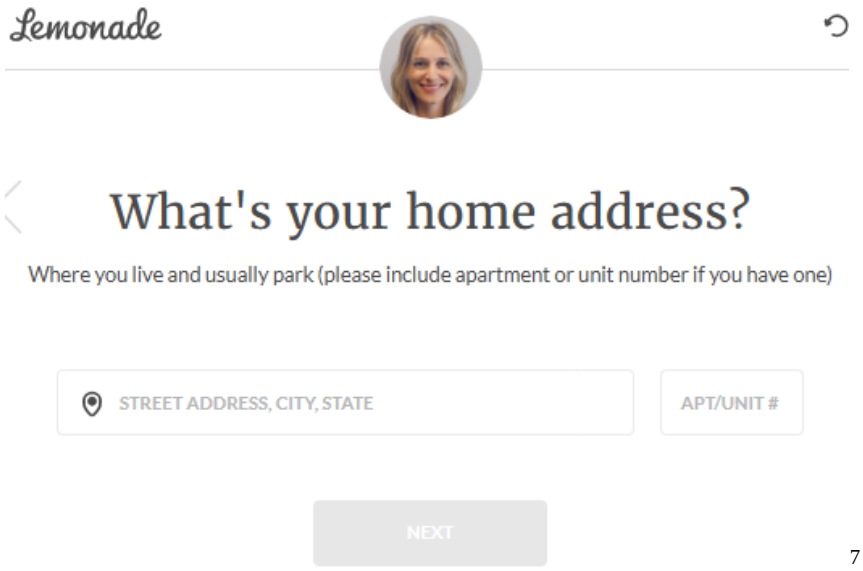


[5]



[6]

[5] https://www.lemonade.com/onboarding/1
[6] https://www.lemonade.com/car/1?f=1



[7]

32. Defendant's quoting feature uses the information entered by the website visitor, combined with additional information Defendant has or that Defendant can access from third-party data brokers, and then automatically displays (commonly referred to as "pre-filling" or "auto-populating") the additional information to the visitor as part of the quote process.

33. Specifically, Defendant's quoting feature asks any visitor to the site for their name, date of birth, and address. Once a visitor enters that information, Defendant's system auto-populates the quotation with driver's license information from Defendant's own databases or from third-party prefill services and makes that information visible to the person entering the information on the Defendant's Quote Platform. A person's name, date of birth, and address are data that are often easily obtained. Defendant knew that this information was often available to the public at no cost, and that cybercriminals are commonly in possession basic data combinations, including name, address and date of birth and can acquire on the dark web huge datasets containing

[7] https://www.lemonade.com/car/2

this information for millions of consumers.[8]

34. Given that Defendant's website functioned as a driver's license lookup tool, scammers used an automated process on Defendant's instant Quote Platform to access Plaintiff's and Class Members' driver's license numbers that Defendant was knowingly and intentionally disclosing through the coding it created for the Quote Platform.

35. The proposed Class includes many people—like Plaintiff—who never applied for insurance with Defendant, were not Defendant's customers, and may not even have been aware of Defendant's existence. In other words, unauthorized parties availed themselves of the PI Defendant made publicly available via its instant Quote Platform on a wholesale basis.

36. Defendant's Quote Platform did not require verification that the person or automated process accessing the system was actually the individual for whom the information was being entered. In addition, Defendant's Quote Platform did not employ effective, industry-standard security measures to detect whether the website visitor was, in fact, a "bot" or automated process rather than an individual person. Instead, Defendant knowingly and intentionally configured its online Quote Platform to provide PI—including driver's license numbers—when anyone, including bots, merely entered basic information such as a person's name, date of birth, and address. Thus, Defendant's Quote Platform was purposefully and knowingly created to allow any site visitor, including bots, to access and view PI including driver's license numbers of anyone

[8] For example, "[s]ince approximately 2009, MyLife has purchased public record data about individuals from data brokers. … MyLife uses that data to create a 'public listing' or profile for these individuals, which can be accessed through its website, www.mylife.com. … On its website, MyLife has profiles purporting to cover at least 320 million individuals. ... Information that may be available through a *free search may include: name; city and state of residence; … email address, and mailing address associated with the profile; date of birth*; …." *United States v. MyLife.com, Inc.*, No. CV 20-6692-JFW(PDX), 2021 WL 4891776, at *2 (C.D. Cal. Oct. 19, 2021) (citations omitted) (emphasis added).

about whom Defendant had collected or could access that PI simply so that Defendant could more easily sell its main product.

B. Defendant Contravened the Purpose of the Driver's Privacy Protection Act

37. Prior to the enactment of the DPPA, Congress found that most states freely turned over DMV information to whomever requested it with few restrictions. 137 Cong. Rec. 27,327 (1993).

38. Due to this lack of restrictions, Congress grew concerned that potential criminals could easily obtain the private information of potential victims. 140 Cong. Rec. 7929 (1994) (statement of Rep. Porter Goss).

39. These concerns did, in fact, materialize in the occurrence of crime, harassment, and stalking. Most notably, in 1989, a stalker shot and killed Rebecca Schaeffer, an up and coming actor, after obtaining her unlisted home address from the California DMV. 137 Cong. Rec. 27,327 (1993). In advocating for the DPPA, Representative Jim Moran (D-VA) recounted thieves using information from the DMV to learn home addresses and commit burglary and theft. 137 Cong. Rec. 27,327 (1993). Similarly, Senator Barbara Boxer (D-CA) explained how a man used the DMV to obtain the home addresses of several young women and sent them harassing letters. 39 Cong. Rec. 29,466 (1993). In another instance, a woman who visited a clinic that performed abortions found black balloons outside her home after a group of anti-abortion activists sought to harass her upon seeing her car in the clinic's parking lot. 139 Cong. Rec. 29,462 (1993) (statement of Sen. Chuck Robb).

40. In response to public outrage over the Schaeffer murder and growing concern for the threat to public safety that free access to DMV records posed, Congress enacted the DPPA "to protect the personal privacy and safety of licensed drivers consistent with the legitimate needs of

business and government." S. Res. 1589, 103rd Cong. §1(b), 139 Cong. Rec. 26,266 (1993) (enacted).

41. Additionally, in enacting the DPPA, Congress was motivated by its "[c]oncern[] that personal information collected by States in the licensing of motor vehicle drivers was being released – even sold – with resulting loss of privacy for many persons." *Akkawi v. Sadr*, No. 2:20-CV-01034-MCE-AC, 2021 WL 3912151, at *4 (E.D. Cal. Sept. 1, 2021) (citing *Maracich v. Spears*, 570 U.S. 48, 51–52 (2013) (alterations in original)). The release of private information like driver's license numbers and other motor vehicle records was the exact impetus for the DPPA's passage.

42. Congress sought to expressly prohibit "disclosing personal information obtained by the department in connection with a motor vehicle record." *Chamber of Com. of United States v. City of Seattle*, 274 F. Supp. 3d 1140, 1154 (W.D. Wash. 2017). Driver's license numbers are thus explicitly listed as "personal information" from "motor vehicle records" under the DPPA. *See* 18 U.S.C. 2725(1), (3). As such, Congress used its lawmaking authority to properly elevate the disclosure driver's license numbers and other motor vehicle records into a concrete harm, a harm that bears a sufficiently close relationship to the tort of public disclosure long recognized at common law.

43. By knowingly using the PI of Plaintiff and the Class for sales and marketing purposes, and by knowingly disclosing that PI to the public, Defendant ran afoul of the purpose of the DPPA, and threatened the privacy and safety of licensed drivers, for whose protection the statute was enacted. Defendant's actions constituted a concrete injury and particularized harm to Plaintiff and members of the Class, that would not have happened but for Defendant's failure to

adhere to the DPPA. Plaintiff was harmed by the public disclosure of his PI in addition to the other harms enumerated herein.

C. The Data Use and Disclosure, and Its Impact

44. In its Notice, Defendant informed consumers that their sensitive PI—namely, driver's license numbers—was compromised in a security incident, which it described as follows:

> Through certain of its subsidiaries, Lemonade offers car insurance policies through an online application process at www.lemonade.com/car (the "Online Flow"). Using the Online Flow to obtain an insurance quote and purchase a policy, an individual enters certain information – name, date of birth, and residential address. On March 24, 2025, we learned that due to a vulnerability in our Online Flow, certain driver's license numbers for identifiable individuals were likely exposed.
>
> Lemonade believes that the unauthorized exposures spanned from approximately April 2023 through September 2024.

45. While the Notice indicates that Defendant "promptly took steps to eliminate the vulnerability," the notice also makes clear that Defendant failed to discover the Data Disclosure for *17 months* while it remained ongoing, and failed to detect it for *two years*.

46. Defendant's use of the driver's license numbers, its Data Disclosure through its online Quote Platform, and its violation of the law—including the DPPA—assisted an ongoing and concerted campaign by fraudsters to engage with insurers' Quote Platforms to obtain driver's license numbers to perpetuate known occurrences of fraud and identity theft.

47. On February 16, 2021, the New York State Department of Financial Services ("DFS") issued an alert regarding an ongoing systemic and aggressive campaign to engage with public-facing insurance websites—particularly those that offer instant online automobile insurance quotes like Defendant's website—to obtain non-public information, in particular unredacted driver's license numbers.[9] According to the alert, the unauthorized collection of driver's license

[9] N.Y. DEPARTMENT OF FINANCIAL SERVICES, *Industry Letter* (Feb. 16, 2021),

numbers appeared to be part of a growing fraud campaign targeting pandemic and unemployment benefits. DFS first became aware of the campaign when it received reports from two auto insurers in December 2020 and January 2021 that cybercriminals were targeting their websites that offer instant online automobile insurance quotes to obtain unredacted driver's license numbers.

48. Insurers' instant online auto quoting websites are the primary entry point for cybercriminals to access consumers' PI. As the industry has accelerated adoption of faster-quoting processes and tools to achieve competitive advantage, new vulnerabilities have opened.[10] According to DFS, insurers noticed an unusually high number of abandoned quotes or quotes not pursued after the display of the estimated insurance premium. On the instant quote websites, "criminals entered valid name, any date of birth and any address information into the required fields" and "then displayed an estimated insurance premium quote along with partial or redacted consumer [PI] including a driver's license number. The attackers captured the full, unredacted driver's license numbers without going any further in the process and abandoned the quote."[11] Of course, Defendant need not use driver's license numbers on a sales platform, or disclose this information to the public, to underwrite any auto insurance policy.

49. In January 2021, DFS alerted approximately a dozen entities maintaining such websites that they were likely targets of unauthorized third-parties looking to gain access to New Yorkers' PI, specifically driver's license numbers. Following the alert, six more insurers apparently reported to DFS the malicious targeting of their websites—two of which insurers reported that the fraudsters failed to gain access to PI, and four of which reported that the fraudsters

---

https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert#_edn (last visited June 6, 2025).

[10] *Id.*

[11] *Id.*

did gain access to PI or that their investigation was still ongoing. In the alert, DFS did not name the websites affected or the insurers.

50. The DFS issued a second alert on March 30, 2021, urging companies like Defendant to avoid displaying prefilled driver's license numbers "considering the serious risk of theft and consumer harm."[12]

51. The increase in interest in driver's license numbers is, in part, a product of the changes brought on by the COVID-19 pandemic, as various types of financial transactions that used to be conducted exclusively in person have been transferred online. Some states are also allowing residents to use expired driver's licenses for various purposes for an extended period, due to difficulty in securing the in-person DMV appointments necessary to renew them.[13]

52. Unsurprisingly, fraudulent unemployment claims spiked during the pandemic, as more money became available to displaced workers and the requirements for filing eased. Many states even paid out tens of millions of dollars to scammers, a phenomenon largely driven by the unauthorized use of fraudulently obtained PI. Threat actors have been caught using not just sensitive personal data for these fraudulent unemployment claims, but also hacking into existing unemployment accounts to change bank payment information.[14]

---

[12] N.Y. DEPARTMENT OF FINANCIAL SERVICES, *Industry Letter* (Mar. 30, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210330_cyber_alert_followup (last visited June 6, 2025).

[13] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO MAGAZINE (Apr. 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited June 6, 2025).

[14] *Id.*

53. The United States Department of Labor estimates that pre-pandemic fraudulent unemployment claims accounted for about 10% of all filings.[15] A normal yearly cost for fraudulent unemployment claims is about $3 billion; recent reports indicate that this number ballooned to $200 billion during the pandemic. Fraudulent first-time claims drove a lot of this activity, but experts expect the problem to persist even as most Americans head back to work. Some will fail to notify the state unemployment office of their change in employment status, creating an opening for scammers.

54. Defendant knew that it was using driver's license information on its online sales Quote Platform. Defendant also knew that this platform was created and maintained in a way that allowed fraudsters to plug in readily, publicly available basic PI of other persons, and that the website would auto-populate driver's license information once that basic information was entered. Indeed, Defendant was responsible for its Quote Platform, including its design and design features. Defendant thus knew or should have known, that its website and the website's auto-populate feature disclosed consumers' driver's license number to unauthorized third parties. This is exactly how Defendant designed its website to operate. Not only did Defendant know that it was using driver's license numbers to sell insurance, and that it was disclosing driver's license numbers to the public, but it also failed to assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumers' PI, and failed to implement basic safeguards to protect the security, confidentiality, and integrity of that information. By adding the auto-population feature to its Quote Platform, which Defendant knowingly and intentionally chose to do, Defendant intended to use the driver's license numbers and make the returned information

[15] Megan DeMatteo, *Unemployment fraud costs victims $200 billion annually in the U.S. – here's how to protect yourself,* CNBC (Dec. 3, 2023), https://www.cnbc.com/select/how-to-protect-yourself-from-unemployment-fraud/ (last visited June 6, 2025).

easily accessible to anyone who entered basic information into its system. Defendant did not impose any security protocols to ensure that website visitors entered and accessed PI only about themselves. Defendant did not impose effective security protocols to prevent automated bots from accessing consumers' PI. Thus, Defendant knowingly used and posted consumers' driver's license numbers directly to all members of the public through its knowing, intentional creation of its Quote Platform and the functionality it designed and implemented therein.

D. Defendant Acknowledged That the Use of Data and its Data Disclosure Created a Substantial Risk of Identity Theft and Fraud

55. The extent, scope, and impact of Defendant's use of the data and its Data Disclosure on its customers and other consumers remains uncertain. Nevertheless, the harm caused to Plaintiff and Class Members by Defendant's use of the information and its Data Disclosure is already apparent. Criminals now possess Plaintiff's and Class Members' driver's license numbers, and its only purpose in obtaining and possessing that information is to monetize that data by selling it on the darknet or dark web or using it to commit other types of fraud.

56. Defendant's Notice puts the burden on Plaintiff and Class Members to take mitigating steps to protect their information: "remain vigilant with respect to reviewing your account statement and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities" and explains how to obtain one's credit reports, including initiating a credit freeze, checking the consumer's credit report, and enrolling in identity theft insurance.

57. Having received the Notice about this Data Disclosure, it is reasonable for Plaintiff and Class Members to believe that the risk of future harm (including identity theft or fraud) is substantial and imminent, and to take steps to mitigate that substantial risk of future harm. Defendant's specific instructions and warnings in the Notice relate to the fact that threat actors

take driver's license numbers for the purpose of committing fraud in the name of the person whose license number is taken.

E. The PI Defendant Obtained, Used and Then Disclosed in its Data Disclosure is Highly Valuable to Fraudsters

58. It is well known amongst companies that store or have access to sensitive PI that driver's license numbers are valuable and frequently targeted by criminals. The PI that Defendant voluntarily disclosed via its Quote Platform in violation of state and federal law is very valuable to phishers, identity thieves, cyber criminals, and other fraudsters, especially as an unprecedented numbers of criminals are filing fraudulent unemployment benefit claims, and driver's license information is uniquely connected to the ability to file such claims and commit other financial fraud. Unsecured sites that contain or transmit PI like driver's license numbers require notice to consumers when the data is stolen because it can be used to commit identity theft and other types of fraud.

59. The driver's license numbers disclosed in Defendant's Data Disclosure are significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. By contrast, the information disclosed in Defendant's Data Disclosure can be used to *open* fraudulent bank accounts and credit and debit cards, or to take out loans, especially student loans. The driver's license numbers disclosed in Defendant's Data Disclosure are also more valuable because they are long lasting, and difficult (if not impossible) to change.

60. With access to an individual's driver's license number, criminals can commit all manner of fraud, including: obtaining government benefits in the victim's name, filing fraudulent tax returns using the victim's information, or obtaining a driver's license or official identification card in the victim's name but with the thief's picture. In addition, identity thieves may obtain a

job, rent a house, or receive medical services in the victim's name, and may even give the victim's driver's license number during an arrest, resulting in an arrest warrant being issued in the victim's name.[16] They can also use the driver's license when receiving a ticket or to provide to an accident victim, to replace or access account information on social media sites, to obtain a mobile phone, to dispute or approve a SIM swap, to redirect U.S. mail, to gain unauthorized access to the United States, to claim a lost or stolen passport, to use as a baseline to obtain a Commercial Driver's License, or to engage in phishing or other social engineering scams.

61. Fraudsters often aggregate information taken from data security incidents to build profiles on individuals. These profiles combine publicly available information with information discovered in previous data security incidents and exploited vulnerabilities. Unique and persistent identifiers such as Social Security numbers, driver's license numbers, usernames, and financial account numbers (e.g., credit cards, insurance policy numbers, etc.) are critical to forging an identity. When not all information is available, the information that is stolen is used to socially engineer a victim into providing additional information so a "full"[17] profile can be obtained.

62. There is no legitimate or legal reason for anyone to use Defendant's website to acquire driver's license information on Plaintiff and the Class Members. Dark Net Markets ("DNM(s)"), or the "dark web," is a heavily encrypted part of the internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity. When malicious actors obtain ill-gotten PI, that information often ends up on the dark web because the

[16] *See* FEDERAL TRADE COMMISSION, *Warning Signs of Identity Theft*, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited on June 6, 2025).

[17] "Fullz" is slang used by threat actors and various criminals meaning "full information," a complete identity profile or set of information for an entity or individual.

malicious actors buy and sell that information for profit.[18] "Why else would hackers . . . steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015).

63. Any non-public data, especially government issued identification numbers like a driver's license or non-driver's identification number, has criminal value.[19] For example, a fake U.S. citizenship kit for sale—passport, Social Security Number, driver's license, and birth certificate—is offered on the dark web for 0.218 bitcoin (or $1,400 at the time) and a stolen/fake driver's license (by U.S. state) for $200.[20]

64. In some ways, driver's license numbers are even more attractive than Social Security numbers to threat actors and more dangerous to the consumer when disclosed. Unlike a Social Security number, a driver's license number is not monitored as closely, so it can potentially be used in ways that will not immediately alert the victim. Threat actors know this as well. Because driver's licenses contain, or can be used to gain access to, uniquely qualifying and comprehensive identifying information such as eye color, height, weight, sex, home address, medical or visual restrictions, and living will/health care directives, most insurance and credit agencies highly recommend immediate notice and replacement, and that identity theft protections are put in place

---

[18] IDENTITY FORCE, *Shining a Light on the Dark Web with Identity Monitoring*, Feb. 1, 2020, https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited June 6, 2025).

[19] IDENTITY THEFT RESOURCE CENTER, *Can Someone Steal Your Identity From Your Driver's License?*, April 16, 2025, https://www.idtheftcenter.org/can-someone-steal-your-identity-from-your-drivers-license/ (last visited June 6, 2025).

[20] Daniel Shkedi, *Heart of Darkness: Inside the Darknet Markets that Fuel Financial Cybercrime*, BIOCATCH, https://web.archive.org/web/20210905231044/https://www.biocatch.com/blog/financial-cybercrime-darknet-markets (last visited Apr. 8, 2024).

for a minimum of three years. Most cybersecurity experts, including Enterprise Knowledge Partners, recommend five years or more.

65. Blogger John Egan from the national credit reporting company Experian emphasized the value of driver's license information to thieves and cautioned:

> Your stolen driver's license number can be the key to unlock all sorts of fraud, such as opening financial accounts in your name or creating fake IDs. [If] stolen in a data breach. . . it can wreak havoc on your finances.[21]

66. In fact, according to the data privacy and cyber security publication CPO Magazine:

> To those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation. Tim Sadler, CEO of email security firm Tessian, points out why this is not the case and why these numbers are very much sought after by cyber criminals: ". . . It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks. . . . bad actors may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar. . . . In other cases, a scam using these driver's license numbers could look like an email that impersonates the DMV, requesting the person verify their driver's license number, car registration or insurance information, and then inserting a malicious link or attachment into the email."[22]

67. Further, an article on TechCrunch explains that it is driver's license or non-driver's identification numbers themselves that are the critical missing link for a fraudulent unemployment benefits application:

> Many financially driven criminals target government agencies using stolen identities or data. But many U.S. states require a government ID — like a driver's

---

[21] John Egan, *What Should I Do If My Driver's License Number Is Stolen?*, EXPERIAN (June 13, 2024) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited June 6, 2025).

[22] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO MAGAZINE (Apr. 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited June 6, 2025).

> license — to file for unemployment benefits. To get a driver's license number, fraudsters take public or previously breached data and exploit weaknesses in auto insurance websites to obtain a customer's driver's license number. That allows the fraudsters to obtain unemployment benefits in another person's name.[23]

68. The use of stolen driver's license numbers to obtain unemployment benefits under another person's name was confirmed by the New York State DFS on February 16, 2021, in its industry letter described above, which stated that they had "recently learned of a systemic and aggressive campaign to exploit cybersecurity flaws in public-facing websites to steal [PI, including] websites that provide an instant quote …. [and that] DFS has confirmed that, at least in some cases, this stolen information has been used to submit fraudulent claims for pandemic and unemployment benefits."[24]

69. The process that was used to extract the data from Defendant's website was likely automated. The identity thieves have demonstrated the value they place on the driver's license numbers by engaging in a systematic and businesslike process for collecting them from Defendant's Data Disclosure and from additional insurers' websites offering instant quotes.

70. The United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that, when criminals use PI to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name, this type of identity fraud can be the most harmful because it may take some time for a victim to become

---

[23] Zach Whittaker, *Geico Admits Fraudsters Stole Customers' Driver's License Numbers for Months*, TECHCRUNCH (Apr. 19, 2021), https://techcrunch.com/2021/04/19/geico-driver-license-numbers-scraped/#:~:text=To%20get%20a%20driver's%20license,benefits%20in%20another%20person's%20name (last visited June 6, 2025).

[24] N.Y. DEPARTMENT OF FINANCIAL SERVICES, *Industry Letter* (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert#_edn (last visited June 6, 2025).

aware of the fraud, and can adversely impact the victim's credit rating in the meantime.[25] The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[26]

F. Defendant Failed to Comply with Federal Trade Commission Requirements

71. Federal and state governments established security standards and issued recommendations to minimize unauthorized data disclosures, and knowing disclosures of information via public websites, and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[27]

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[28] Among other things, the guidelines note businesses should properly dispose of PI that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to

---

[25] *See* UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, June 2007, http://www.gao.gov/assets/270/262899.pdf (last accessed June 6, 2025).

[26] *Id.*

[27] FEDERAL TRADE COMMISSION, *Start With Security: A Guide for Business*, June 2015, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed June 6, 2025).

[28] *See* FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business*, Oct. 2016, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed June 6, 2025).

hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[29]

73. Also, the FTC recommends companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify third-party service providers have implemented reasonable security measures.[30]

74. Highlighting the importance of protecting against these types of disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PI, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet its Data security obligations.[31]

75. Through negligence in designing and implementing its online Quote Platform and securing Plaintiff's and Class Members' PI, Defendant knowingly allowed the public—and thieves—to utilize its online Quote Platform to obtain access to and collect individuals' PI. Defendant failed to employ reasonable and appropriate measures to protect against unauthorized disclosure and access to Plaintiff's and Class Members' PI. Defendant's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, and violate the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. § 6801.

---

29 *Id.*

30 *Start With Security*, *see supra* n.35.

31 *See* FEDERAL TRADE COMMISSION, *Privacy and Security Enforcement: Press Releases*, available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last accessed June 6, 2025).

G. Plaintiff's Injuries: Attempts to Secure PI After Defendant's Data Disclosure

76. Defendant admitted in the Notice that it disclosed Plaintiff's and Class Members' driver's license numbers to unauthorized third parties. Defendant tasked Plaintiff and Class Members with various mitigation steps and offered a year of credit monitoring. These measures are woefully inadequate and do not absolve Defendant of its violations of the DPPA and other laws alleged herein.

77. Plaintiff and Class Members have been, and will continue to be, injured because Defendant disclosed their PI, and—per Defendant's instructions— they are now forced to spend time monitoring their credit and governmental communications guarding against identity theft, and resolving fraudulent claims and charges because of Defendant's actions and/or inactions.

H. Plaintiff and Class Members Suffered Additional Damages

78. Plaintiff and Class Members are at risk for actual identity theft in addition to all other forms of fraud.

79. The ramifications of Defendant's disclosure and failure to keep individuals' PI secure are long lasting and severe. Once PI is disseminated to unauthorized parties, fraudulent use of that information and damage to victims may continue for years.[32]

80. Plaintiff's and Class Members' driver's license numbers are private, valuable, and sensitive in nature as they can be used to commit a lot of different harms and fraud in the hands of the wrong people. Defendant did not obtain Plaintiff's and Class Members' consent to disclose such PI to any other person, as required by applicable law and industry standards.

---

[32] LEXISNEXIS RISK SOLUTIONS, *True Cost of Fraud Studies*, https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study (last visited June 6, 2025).

81. Defendant's decision to expose Plaintiff and Class Members to the possibility that anyone, especially thieves with various pieces of individuals' PI, could obtain any individual's driver's license number by utilizing Defendant's front-facing online instant quote platform left Plaintiff and Class Members with no ability to protect their sensitive and private PI.

82. Defendant had the resources necessary to prevent its Data Disclosure, but did not implement data security measures, despite its obligations to protect Plaintiff's and Class Members' PI from unauthorized disclosure.

83. Defendant failed to take reasonable steps to adequately secure Defendant's website and publish it in a manner that did not hand over Plaintiff's and Class Members' driver's license numbers to unauthorized third parties, leaving Defendant's customers and other consumers, including Plaintiff and Class Members, exposed to risk of fraud and identity theft.

84. Defendant was, and at all relevant times has been, aware that the PI it handles and stores in connection with its services is highly sensitive. Because Defendant is a company that provides insurance services involving highly sensitive and identifying information, Defendant was aware of the importance of safeguarding that information and protecting its websites, systems, and products from security vulnerabilities.

85. Defendant was aware, or should have been aware, of regulatory and industry guidance regarding data security, and it was alerted to the risk associated with knowingly providing driver's license numbers to members of the public on Defendant's website.

86. Defendant knowingly obtained, used, disclosed, and compromised Plaintiff's and Class Members' PI by creating the Quote Platform with an auto-populate feature, voluntarily transmitting PI to any member of the public, including fraudulent actors. Defendant failed to take reasonable steps against an obvious threat. Defendant designed and implemented its own website

Quote Platform, which included the instant quote feature that auto-populated Plaintiff's and Class Members' driver's license numbers in response to the input of basic publicly available consumer information, was a feature that Defendant knowingly and intentionally included on its website. Had Defendant never used the information to sell auto insurance or never included this feature on its sales Quote Platform, it would have prevented the disclosure, unauthorized access, and ultimately, the prospective fraudulent use and possible fraudulent use of consumers' PI.

87. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of Defendant's Data Disclosure on their lives.

88. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[33]

89. As a result of Defendant's Data Disclosure, Plaintiff and Class Members have suffered, will suffer, and are at imminent risk of suffering:

a. The compromise, publication, fraudulent, and/or unauthorized use of their PI,

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud,

c. Lost opportunity costs and wages and loss of productivity associated with efforts expended from addressing and attempting to mitigate the actual and future consequences of Defendant's Data Disclosure, including but not limited

[33] U.S. DEPARTMENT OF JUSTICE OFFICE OF JUSTICE PROGRAMS BUREAU OF JUSTICE STATISTICS, *Victims of Identity Theft 2012*, https://www.icpsr.umich.edu/web/NACJD/studies/34735/datadocumentation (last accessed June 6, 2025).

to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud,

d. The continued risk to their PI, which remains in the possession of Defendant and is subject to further compromise so long as Defendant fails to undertake appropriate measures to protect the PI in their possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of Defendant's Data Disclosure for the remainder of the lives of Plaintiff and Class Members.

90. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their PI is secure, remains secure, and is not subject to further disclosure, misappropriation, and theft.

91. To date, other than providing 12 months of credit monitoring and identity protection services, Defendant does not appear to be taking any measures to assist Plaintiff and Class Members other than simply telling them to "remain vigilant with respect to reviewing your account statement and credit reports." This recommendation, however, does not require Defendant to expend any effort to protect Plaintiff's and Class Members' PI; moreover, Defendant fails to provide monetary compensation and provides no protection whatsoever after 12 months.

92. Defendant's disclosure of Plaintiff's and Class Members' driver's license numbers directly to members of the public with small amounts of their PI has resulted in Plaintiff and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Indeed, as Defendant's Notice indicates, it is explicitly *instructing*—and putting the burden on—Plaintiff and Class Members to monitor and discover possible fraudulent activity and identity theft.

93. Defendant's offer of 12 months of identity monitoring and identity protection services to Plaintiff and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come.

94. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen PI for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

95. There may be a time lag between when additional harm occurs versus when it is discovered, and also between when PI is acquired and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[34]

96. As a result of the events detailed herein, Plaintiff and Class Members suffered harm and loss of privacy, and will continue to suffer future harm, because of Defendant's Data Disclosure and the fact that their driver's license numbers are now in the hands of criminals, including but not limited to: invasion of privacy; loss of privacy; loss of control over PI and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of PI; harm resulting from damaged credit scores and credit information; a substantially increased risk of future identity theft and fraud; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized disclosure of PI.

I. Plaintiff Rich's Experience

97. Plaintiff Rich does not currently (and has never had) any insurance policies with

[34] *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, at 29, *see supra* at n.33 (emphasis added).

Lemonade, nor has he ever applied for insurance—or engaged in any other business—with Lemonade.

98. Notwithstanding, Lemonade sent Plaintiff Rich a letter dated April 10, 2025, informing him that Lemonade disclosed his driver's license number to unauthorized third parties through Lemonade's Quote Platform. The letter stated as follows:

> Through certain of its subsidiaries, Lemonade offers car insurance policies through an online application process at www.lemonade.com/car (the "Online Flow"). Using the Online Flow to obtain an insurance quote and purchase a policy, an individual enters certain information—name, date of birth, and residential address. Using this information, Lemonade calls for and returns from its third-party vendor that individual's driver's license number. On March 14, 2025, we learned that due to a vulnerability in our Online Flow, certain driver's license numbers for identifiable individuals were likely exposed. Lemonade believes that the unauthorized exposures spanned from approximately April 2023 through September 2024 …. Based on our investigation, your driver's license number may have been accessed without authorization.

99. In October and November 2024, Plaintiff Rich learned that cybercriminals fraudulently applied for multiple auto loans, on multiple occasions, with multiple lenders, all in his name.

100. Specifically, Ally Bank sent Plaintiff Rich a letter dated October 24, 2024, informing him that an application for an auto loan was made in his name with CarMax, but denied. Plaintiff Rich contacted CarMax on or about November 5, 2024, and was informed that they would investigate the matter, but he never heard anything further from Ally Bank or CarMax.

101. Further, Plaintiff Rich received seven separate letters from Capital One, dated October 18 and 25, 2024 and November 7, 2024, each of which stated that an auto loan application was submitted in his name, but all seven letters contained separate reference numbers, indicating that cybercriminals made seven separate applications for auto loans in his name—four of which were made on the same day. Plaintiff Rich contacted Capital One on or about October 28, 2024,

to report the fraud, and Capital One informed him that it would investigate the situation, but Plaintiff Rich never heard anything further from Capital One.

102. Global Lending Services sent Plaintiff Rich two separate letters dated November 4 and 12, 2024, informing him that two separate applications for auto loan were made in his name, but both were declined. Plaintiff Rich had never applied for either of those auto loans or otherwise heard of Global Lending Services. On November 13, 2024, Plaintiff Rich contacted Global Lending Services to inform them that the loan applications were fraudulent. Global Lending Services instructed Plaintiff Rich to contact Capital One, which is the lender that declined the auto loan applications (Global Lending Services is a third-party intermediary that matches loan applicants with lenders). Plaintiff Rich then contacted Capital One to dispute the loan applications.

103. On or about December 12, 2024, Plaintiff Rich experienced a fraudulent charge for Uber in the amount of $9.99, on his Chase Freedom Visa credit card. Plaintiff Rich does not use Uber, so he contacted Chase to dispute the charge, which Chase promptly reversed. Chase also issued Plaintiff Rich a replacement credit card.

104. On or about November 6, 2024, Plaintiff Rich discovered that a series of fraudulent trades were made on his IRA account with Fidelity. Specifically, on November 7, 2024, unauthorized individuals sold Plaintiff Rich's investments in the S&P 500 Mutual Fund and used the proceeds of the sale to make a series of trades in penny stocks. Plaintiff Rich was forced to take a day off from work on November 6, 2024, to investigate the fraud and contact Fidelity to report and troubleshoot it. Although Plaintiff Rich did not lose any wages as a result, he would have spent that paid-day-off on more valuable endeavors. On or about December 20, 2024, Fidelity reversed those trades.

105. The foregoing fraudulent misuse of Plaintiff Rich's sensitive information is

temporally and logically connected to the data derived from Lemonade's Data Disclosure in the same way that data breach and other privacy cases have found to be "fairly traceable." Lemonade disclosed Plaintiff Rich's driver's license number shortly before he experienced this fraud.

106. Plaintiff Rich has spent and continues to spend considerable time and effort, and has taken and continues to take considerable precautions, to monitor for and protect against the unauthorized dissemination of his driver's license number. To date, he has spent approximately 20-30 hours monitoring accounts and otherwise dealing with the fallout of the Data Disclosure. Unfortunately, because of Lemonade's practice of unlawfully obtaining, using, and disclosing his driver's license number, Plaintiff Rich's sensitive information was disseminated without his consent, is at high risk of being fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

107. Plaintiff Rich is very careful about sharing his driver's license number and has never knowingly transmitted his driver's license number (or other sensitive information) unencrypted over the internet or any other unsecured source. Further, Plaintiff Rich stores documents containing his sensitive information (including his driver's license number) in a secure location and takes steps to ensure his online accounts are secure and password protected.

108. As a result of Lemonade's Data Disclosure, Plaintiff Rich has suffered—or is at an increased risk of suffering—injury and/or damages, including but not limited to, the unauthorized use of his disclosed driver's license number, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PI; and injury to

his privacy.

109. Additionally, because of Lemonade's Data Disclosure, Plaintiff Rich now faces a substantial risk that unauthorized third parties will further misuse his driver's license number. Indeed, because (1) the Data Disclosure involved unauthorized third parties specifically targeting Lemonade's systems (i.e., the online Quote Platform); (2) the dataset of driver's license numbers the unauthorized third parties obtained from Lemonade's disclosure through its Quote Platform has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the driver's license numbers Lemonade disclosed and the unauthorized third parties obtained in the Data Disclosure are highly sensitive and can be misused for substantially injurious forms of identity and/or fraud such as (*inter alia*) fraudulently applying for and obtaining unemployment benefits or loans and opening bank accounts, Plaintiff Rich has (1) suffered, or is at an increased risk of suffering, unauthorized use of his disclosed driver's license number such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his driver's license number and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Disclosure.

110. Plaintiff Rich experienced all of the foregoing harm and injury as a direct result of Lemonade's knowing and voluntary disclosure of his driver's license number in the Data Disclosure. The monetary relief sought herein by Plaintiff Rich would compensate his for the foregoing redressable injuries. Further, Plaintiff Rich seeks injunctive relief to redress the foregoing injuries and harm, including but not limited to requiring Lemonade to take steps to

monitor for, protect, and/or prevent misuse of his driver's license number that Lemonade disclosed in the Data Disclosure, as well as enact adequate data privacy/security practices.

V. CLASS ALLEGATIONS

111. Plaintiff brings this action on behalf of himself and the following Class pursuant to Federal Rule of Civil Procedure 23(a) and (b):

> **Nationwide Class**: All residents of the United States whose driver's license numbers and other PI was obtained, used, and/or disclosed by Defendant through its Quote Platform or otherwise displayed on its website, including but not limited to during the Data Disclosure.

112. Plaintiff reserves the right to re-define the Class(es) prior to class certification. Plaintiff reserves the right to modify these class definitions as discovery in this action progresses.

113. Excluded from the Class are Defendant and its affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case.

114. **Numerosity**: While the precise number of Class Members has not yet been determined, Defendant's filing with the United States Securities and Exchange Commission states that the Data Disclosure impacted "approximately 190,000 individuals"[35]; therefore, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appear to include at least hundreds of thousands of members who are geographically dispersed.

115. **Typicality**: Plaintiff's claims are typical of Class Members' claims. Plaintiff and all Class Members were injured through Defendant's uniform misconduct, and Plaintiff's claims are identical to the claims of the Class Members they seek to represent. Accordingly, Plaintiff's claims are typical of Class Members' claims.

[35] https://d18rn0p25nwr6d.cloudfront.net/CIK-0001691421/bd19d2fb-41d1-4e83-a381-c246044d769b.pdf

116. **Adequacy**: Plaintiff is an adequate representative of the Class because his interests are aligned with the Class he seeks to represent and he has no conflicts of interest with the Class. Plaintiff's Counsel are competent with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and Plaintiff's Counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiff and Plaintiff's Counsel.

117. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other Class Members' claims. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation also presents a potential for inconsistent or contradictory judgments. Individualized litigation further increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

118. **Commonality and Predominance**: The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

a. whether Defendant engaged in the wrongful conduct alleged herein;

b. whether Defendant knowingly used Plaintiff's and the Class Members' driver's license numbers to promote and sell auto insurance;

c. whether Defendant knowingly obtained Plaintiff's and the Class Members' driver's license numbers;

d. whether Defendant knowingly disclosed Plaintiff's and the Class Members' driver's license numbers;

e. whether Defendant violated the DPPA;

f. whether Defendant's data security practices and the vulnerabilities of Defendant's systems resulted in the disclosure of Plaintiff's and other Class Members' sensitive information;

g. whether Defendant violated Plaintiff's and the Class Members' privacy rights;

h. whether Defendant was negligent or negligent per se when they disclosed the sensitive information of Plaintiff and other Class Members; and

i. whether Plaintiff and Class Members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

119. Given that Defendant engaged in a common course of conduct as to Plaintiff and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

VI. CAUSES OF ACTION

COUNT I
Violation of the Driver's Privacy Protection Act, 18 U.S.C. §§ 2724, *et seq.*
(On Behalf of Plaintiff and the Nationwide Class against Defendant)

120. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

121. Plaintiff brings this claim individually and on behalf of the Nationwide Class.

122. The DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains. . . ." 18 U.S.C. § 2724.

123. The DPPA also restricts the resale and redisclosure of personal information, and requires authorized recipients to maintain records of each individual and the permitted purpose of the disclosure for a period of five years. 18 U.S.C. § 2721(c).

124. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." 18 U.S.C. § 2725(1). Driver's license numbers are motor vehicle records and "personal information" under the DPPA. 18 U.S.C. § 2725(3).

125. Defendant obtains, uses, and discloses motor vehicle records from its customers.

126. Defendant also obtains motor vehicle records directly from state agencies or through resellers (third party prefill services) who sell such records.

127. Defendant knowingly used the above-described information to sell auto insurance on its free online Quote Platform, accessible from www.lemonade.com.

128. Defendant knowingly published the above-described information to the public on its free online Quote Platform, accessible from www.lemonade.com.

129. Defendant knowingly linked its public website to systems and/or networks storing maintaining, and/or obtaining Plaintiff's and Class Members' PI.

130. Defendant had a practice of offering online insurance quotes to applicants long before it incorporated this auto-population feature but added the auto-population feature to its online Quote Platform to gain competitive advantage in its sales process. By adding the auto-population feature to its online Quote Platform, which Defendant knowingly chose to do, Defendant knew that it was using the driver's license information to sell insurance and making the displayed information easily accessible to anyone who entered basic information into its system. Defendant did not impose any security protocols to ensure that website visitors entered and accessed PI only about themselves. Defendant did not impose effective security protocols to prevent automated bots from accessing consumers' PI.

131. During the time period of, at least, April 2023 through September 2024, PI,

including driver's license numbers, of Plaintiff and Class Members, was publicly available and viewable, unencrypted, on Defendant's Quote Platform, and Defendant knowingly obtained, used, and disclosed and/or redisclosed Plaintiff's and Class Members' motor vehicle records and PI to the general public, which is not an authorized use permitted by the DPPA pursuant to 18 U.S.C. §§ 2724, 2721(b), and 2721(c).

132. Pursuant to the allegations herein, Defendant knew or should have known that it obtained, disclosed or re-disclosed, and used PI from a motor vehicle record for a purpose not permitted under the DPPA.

133. By engaging in the conduct described above, Defendant knowingly obtained personal information for a purpose not permitted under the DPPA.

134. By engaging in the conduct described above, Defendant knowingly used personal information for a purpose not permitted under the DPPA.

135. By engaging in the conduct described above, Defendant knowingly disclosed or re-disclosed personal information for a purpose not permitted under the DPPA.

136. As a result of Defendant's acquisition, use, subsequent Data Disclosure, and violations of the DPPA, Plaintiff and putative Class Members are entitled to statutory damages to maximum allowable, actual damages, liquidated damages, and attorneys' fees and costs.

COUNT II
Negligence
(On Behalf of Plaintiff and the Nationwide Class Against Defendant)

137. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

138. Plaintiff brings this claim individually and on behalf of the Nationwide Class.

139. Defendant owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class Members' PI from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, implementing, maintaining, and testing its Data security systems to ensure Plaintiff's and Class Members' PI in Defendant's possession, or that could be accessed by Defendant, was adequately secured and protected.

140. Defendant owed a duty to Plaintiff and the Class Members to adopt, implement, and maintain a process by which they could detect vulnerabilities in its websites and systems in a reasonably expeditious period of time and to give prompt notice in the case of a data security incident, including an unauthorized use of data knowingly disclosed on Defendant's website.

141. Defendant owed a duty of care to Plaintiff and Class Members to provide security, consistent with industry standards, to ensure that its systems and networks—and the personnel responsible for them—adequately protected PI it stored, maintained, used, accessed, and/or obtained.

142. Defendant further assumed the duty to implement reasonable security measures as a result of its general conduct, internal policies, and procedures, in which Defendant states, among other things, that Defendant has a "commitment to protecting your privacy."[36] Through these and other statements, Defendant specifically assumed the duty to comply with industry standards in protecting its customers' and other consumers' PI; and to adopt, implement, and maintain internal standards of data security that met those industry standards.

143. Defendant owed a duty by, on information and belief, entering into agreements with various state Departments of Motor Vehicles, which required it to certify that it will not use motor

[36] https://www.lemonade.com/privacy-policy (last accessed June 6, 2025).

vehicle records in manners inconsistent with the DPPA and will secure the information appropriately.

144. Unbeknownst to Plaintiff and Class Members, they were entrusting Defendant with their PI when Defendant obtained their PI from motor vehicle records directly from state agencies or through resellers or third party prefill services who sell such records. Defendant had an obligation to safeguard Plaintiff's and Class Members' PI and were able to protect against the harm suffered by Plaintiff and Class Members. Instead, Defendant chose to disclose Plaintiff's and Class Members' driver's license numbers so they could sell more auto insurance.

145. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in having its systems auto-populate online quote requests with private PI without the consent or authorization of the person whose PI was being provided. Only Defendant was in a position to ensure that its systems were sufficient to protect against harm to Plaintiff and the Class resulting from a data security incident, instead they chose to disclose Plaintiff's and Class Members' driver's license numbers so they could sell more auto insurance.

146. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PI. Defendant's misconduct included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent disclosure of PI, and instead chose to disclose Plaintiff's and Class Members' driver's license numbers.

147. Defendant acknowledges its conduct created actual harm to Plaintiff and Class Members because Defendant instructed them to monitor their accounts for fraudulent conduct and identity theft, and offered one year of credit monitoring.

148. Defendant knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting PI and the importance of adequate security. Defendant knew about—or should have been aware of—numerous, well-publicized unauthorized data disclosures affecting businesses, especially insurance and financial businesses, in the United States.

149. Because Defendant knew that its disclosure of sensitive PI would damage thousands of individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect its Data systems and the PI contained and/or accessible therein.

150. Defendant breached its duties to Plaintiff and Class Members, and thus were negligent, by designing the Quote Platform and website so that it automatically provided Plaintiff's and Class Members' driver's license information directly to members of the public, failing to recognize in a timely manner that Plaintiff's and Class Members' PI had been disclosed, and failing to warn Plaintiff and Class Members in a timely manner that their PI had been disclosed.

151. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

152. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known it was failing to meet its duties, and the Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the disclosure of their PI.

153. Neither Plaintiff nor the other Class Members contributed to Defendant's Data Disclosure.

154. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class Members have suffered and/or will suffer injury and damages, including but not limited to: (i) the

loss of the opportunity to determine for themselves how their PI is used; (ii) the publication and/or fraudulent use of their PI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of Defendant's Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PI, which remains in Defendant's possession (and/or to which Defendant continue to have access) and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PI in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of disclosed PI.

155. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' PI.

156. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Declaratory and Injunctive Relief
(On Behalf of Plaintiff and the Nationwide Class against Defendant)

157. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

158. Plaintiff brings this claim individually and on behalf of the Nationwide Class.

159. As previously alleged, Plaintiff and Class Members have a reasonable expectation that companies such as Defendant, who could access their PI through automated systems, would provide adequate security for that PI.

160. Defendant owes a duty of care to Plaintiff and Class Members requiring them to adequately secure PI.

161. Defendant still possess and can still access PI regarding Plaintiff and Class Members.

162. Since its Data Disclosure, Defendant has announced few, if any changes to its decision to disclose the PI, its Data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems or Quote Platform.

163. Defendant's Data Disclosure caused actual harm because of Defendant's failure to fulfill its duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PI and Defendant's failure to address the security failings that led to such exposure.

164. There is no reason to believe that Defendant's security measures are more adequate now to meet Defendant's legal duties than they were before its Data Disclosure.

165. Plaintiff therefore seeks a declaration (1) that Defendant's existing security measures do not comply with its duties of care to provide adequate security, and (2) that to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendant not to disclose PI, including driver's license information, to the general public through its website or sales platforms;

b. Ordering Defendant to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated inquiries by bots, simulated cyber-attacks, penetration tests, and audits on

Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors,

c. Ordering Defendant to engage third–party security auditors and internal personnel to run automated security monitoring, including risk analysis on Defendant's decision making,

d. Ordering Defendant to audit, test, and train its security personnel regarding any new or modified procedures,

e. Ordering Defendant not to make PI available on its Quote Platform,

f. Ordering Defendant not to store PI or make PI accessible in any publicly facing website,

g. Ordering Defendant to purge, delete, and destroy in a reasonably secure manner customer and consumer data not necessary for its provisions of services,

h. Ordering Defendant to conduct regular computer system scanning and security checks; and

i. Ordering Defendant routinely and continually to conduct internal training and education to inform employees and officers on PI security risks, internal security personnel how to identify and contain a disclosure when it occurs and what to do in response to a data security incident.

COUNT IV
Violations of New York General Business Law
N.Y. Gen. Bus. Law § 349 ("GBL")
(On Behalf of Plaintiff and the Nationwide Class against Defendant)

166. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

167. Plaintiff brings this cause of action individually and on behalf of the Nationwide Class.

168. Section 349 of the New York GBL provides that "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful." N.Y. Gen. Bus. Law § 349(a).

169. Defendant, while operating in New York, engaged in deceptive acts and practices in the conduct of business, trade and commerce, and the furnishing of services, in violation of N.Y.Gen. Bus. Law § 349(a). This includes but is not limited to the following:

1. disclosing Plaintiff's and Class Members' PI;

2. failing to enact adequate privacy and security measures to protect Plaintiff's and Class Members' PI from unauthorized disclosure, release, and theft;

3. failing to take proper action following known security risks and prior cybersecurity incidents;

4. knowingly and fraudulently providing Plaintiff's and Class Members' driver's license information directly to members of the public with small amounts of their PI;

5. omitting, suppressing, and concealing the inadequacy of Defendant's security protections;

6. knowingly and fraudulently misrepresenting that Defendants would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of PI, and

7. failing to disclose its Data Disclosure to the victims in a timely and accurate manner, in violation of the duties imposed by, inter alia, N.Y. Gen Bus. Law § 899-aa(2).

170. As a direct and proximate result of Defendant's practices, including its Data Disclosure, Plaintiff and other Class Members suffered injury and/or damages, including but not limited to actual misuse of their PI, fraud, and identity theft; lost time and expenses related to monitoring their accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PI.

171. The above unfair and deceptive practices and acts by Defendant was immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and other Class Members that they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

172. In view of its decision to disclose the PI in its Data Disclosure, Defendant knew or should have known that its systems and data security practices were inadequate to safeguard PI entrusted to it, and that risk of fraudsters obtaining the PI was highly likely.

173. Defendant's actions in engaging in the above-named unfair practices and deceptive acts, including Defendant's Data Disclosure, were negligent, knowing and willful.

174. Plaintiff and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including but not limited to actual damages (to be proven at trial), treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

175. Plaintiff and Class Members seek to enjoin such unlawful deceptive acts and practices described above. Each Class Member will be irreparably harmed unless the Court enjoins Defendant's unlawful, deceptive actions, in that Defendant will continue to fail to protect PI entrusted to them, as detailed herein.

176. Plaintiff and Class Members seek declaratory relief, restitution for monies wrongfully obtained, disgorgement of ill-gotten revenues and/or profits, injunctive relief prohibiting Defendant from continuing to disseminate its false and misleading statements, and other relief allowable under N.Y. Gen. Bus. Law § 349.

COUNT V
Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class against Defendant)

177. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

178. Plaintiff brings this cause of action individually and on behalf of the Nationwide Class.

179. Defendant had independent duties under state and federal laws requiring Defendants to reasonably safeguard Plaintiff's and Class Members' PI. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45) and the GLB Act (15 U.S.C. § 6801 *et seq.*), Defendant had a duty to provide adequate data security practices in connection with safeguarding Plaintiff's and Class Members' PI. Further, pursuant to the Federal Trade Commission Act (15 U.S.C. § 45) and N.Y. Gen. Bus. Law § 349, Defendants had a duty to provide fair, reasonable, or adequate data security in connection with the sale of insurance policies and use of the Defendant's website in order to safeguard Plaintiff's and Class Members' PI.

180. Finally, pursuant to DPPA, 18 U.S.C. § 2724, *et seq.*, Defendant had a duty (but failed) to protect and also to refrain from knowingly obtaining, disclosing, or using protected motor vehicle record information for impermissible purposes, and reselling, redisclosing, or—as recipients of the information—improperly maintaining protected motor vehicle record information. 18 U.S.C. §§ 2721, 2724. The DPPA states that "[i]t shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title." 18 U.S.C. § 2722(a). The DPPA also states that "[a] State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity: personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section." 18 U.S.C. § 2721(a)(1). Defendant failed to abide by, and thus violated, the DPPA.

181. Defendant violated the DPPA by intentionally configuring and designing its insurance quote application portal on its website to disclose Plaintiff's and Class members' PI to anyone who requested an insurance quote. Defendant installed no protections or security measures

to protect this information and willfully disclosed it to cyber criminals through the intentional configuration and design of its insurance quote application portal. Defendant's conduct was particularly unreasonable given the nature and amount of PI it obtained and disclosed and the foreseeable consequences of a data disclosure.

182. In engaging in the knowing and/or negligent acts and omissions as alleged herein, in which Defendant disclosed Plaintiff's and Class Members' PI to malicious actors through its online sales system, Defendant violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce," and the GLB Act. This includes failing to have adequate data security measures and failing to protect Plaintiff's and the Class Members' PI. Defendant also breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45) and N.Y. Gen. Bus. Law § 349, among other statutes, by failing to provide fair, reasonable, or adequate data security in order to safeguard Plaintiffs' and Class Members' PI in connection with the use of the Defendant's website and online sales system. Defendant violated the DPPA by knowingly obtaining, using, and disclosing and/or redisclosing Plaintiff's and Class Members' motor vehicle records and PI to the general public in a manner that did and does not constitute authorized use permitted by the DPPA pursuant to 18 U.S.C. §§ 2724, 2721(b), and 2721(c), among other violations of the DPPA alleged herein.

183. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

184. Plaintiff and Class Members are within the class of persons that the DPPA, the GLB Act, and the FTC Act were intended to protect. The DPPA was expressly designed to protect a person's personal information contained in motor vehicle records from unauthorized disclosure.

The GLB Act was expressly designed to protect private and personal information. The FTC Act are consumers designed to be protected by Section 5.

185. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

186. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it were failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PI.

187. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members now face an increased risk of future harm. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

VII. PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Class, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as the class representative and Plaintiff's Counsel as class counsel;

B. Award Plaintiff and Class Members actual, statutory, punitive, monetary, and nominal damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class Members have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Award Plaintiff and Class Members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and Class Members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and Class Members such other favorable relief as allowable under law or at equity.

VIII. JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: June 9, 2025

/s/ Zachary M. Vaughan
Zachary M. Vaughan, SBN 4993283
BERGER MONTAGUE PC
1001 G Street, NW
Fourth Floor, Suite 400 East
Washington DC 20001
Tel: 215.875.4602
Fax: 215.875.4604
Email: zvaughan@bm.net

E. Michelle Drake (*pro hac vice* forthcoming)
BERGER MONTAGUE PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Tel: (612) 594-5999
Fax: (612) 584-4470
Email: emdrake@bm.net

Mark B. DeSanto (*pro hac vice* forthcoming)
BERGER MONTAGUE PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel: (215) 875-3000
Fax: (215) 875-4604
Email: mdesanto@bm.net

Counsel for Plaintiff